业务系统敏感信息防泄漏解决方案

背景与需求分析

2011 年底一连串泄密事件互联网敏感信息泄漏的问题成为众人关注的焦点：

12 月初，国内多家银行的用户数据已经泄露，数据包含了用户的姓名、卡号、密码等敏感信息；

12 月中，某省公安厅出入境政务服务网网上申请数据泄露；

12 月 21 日，CSDN 的用户数据库被黑，600 余万用户资料被泄露。CSDN 在官方微博上证实这一消息，并表示已经报案；

12 月 22 日，人人网 500 万用户资料遭泄露；

12 月 25 日，网传天涯 400 万用户资料泄密，天涯回应称早期曾使用过明文密码，此次被盗的数据为 2009 年之前的备份数据；

12 月 27 日，据乌云漏洞报告平台称，京东商城存在用户权限控制不当漏洞，会导致用户资料完全泄漏，易被第三方获取。

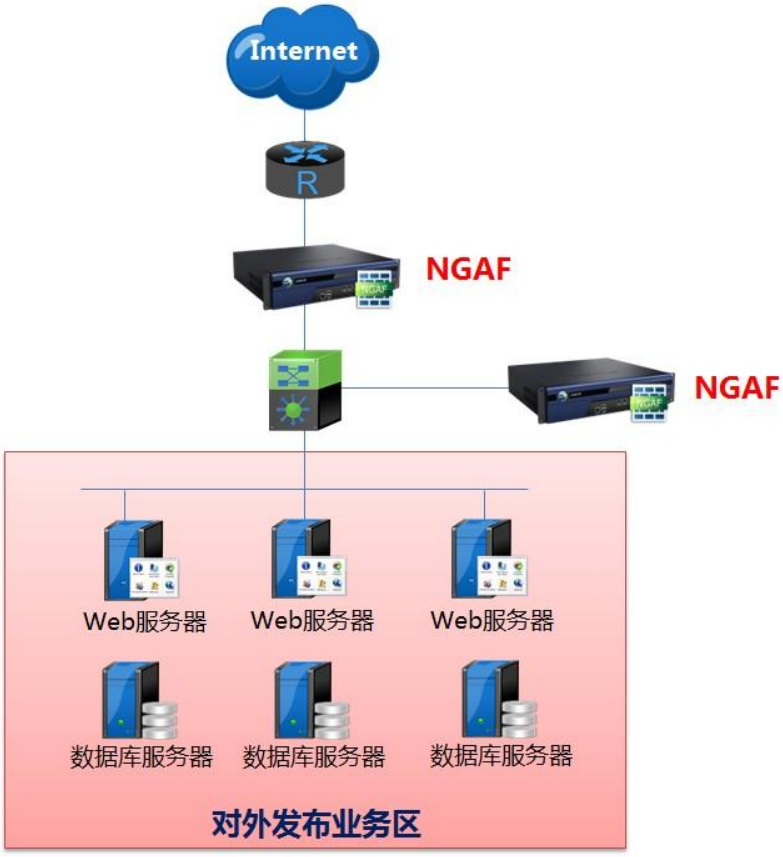
应对上述安全事件，传统的 DLP 数据防泄密解决方案显然很难起到有效的防护效果，此类重大安全事件的产生多是通过正常的 web 业务访问，通过数据库认为合法的操作语句产生“拖库”、“暴库”的安全问题。新的安全风险的产生要求对互联网提供服务的企业、政府完善整体安全框架建设，加强安全管理的同时还需具备双向的内容检测能力：

对外，防止 web 攻击（如注入类攻击）对后端数据库、FTP 等服务器的操作带来的安全问题；例如，需要有效防止黑客通过 SQL 注入攻击找到业务系统漏洞，并通过 SQL 语句将储存在数据库中的敏感信息查看并泄露，产生“拖库”、“暴库”的安全问题。

对内，有效检测交互过程中内容的合法性，具有向外发送的数据内容是否为非法窃取、是否符合正常访问安全逻辑的判断能力。如，业务请求中一个连接查询一条用户信息视为正常，而一次连接造成大量的用户信息外流则可能存在一定的安全风险。

深信服解决之道

深信服提供针对业务系统的敏感数据防泄露解决方案，通过在线部署一台深信服 NGAF 下一代防火墙，从攻击源头上帮助用户防护导致业务系统信息泄露的黑客攻击；通过旁路部署一台深信服 NGAF 下一代防火墙，提供有特征的敏感数据内容的过滤的功能，帮助用户清晰定义数据内容的安全等级，防止敏感数据泄露。



可定义的敏感信息防泄漏

深信服敏感信息防泄漏解决方案可以自定义多种敏感信息内容进行有效识别、报警并阻断，防止大量敏感信息被非法泄露。

- 用户信息
- 邮箱账户信息
- MD5 加密密码
- 银行卡号
- 身份证号码
- 社保账号
- 信用卡号
- 手机号码

……

应用信息隐藏

针对业务系统后台业务系统服务器（如：WEB 服务器、FTP 服务器、邮件服务器等）反馈信息进行了有效的隐藏。防止黑客利用服务器返回信息进行有针对性的攻击。

注入类攻击防护

通过 web 安全防护模块有效防护造成信息泄露的 web 攻击,（如注入类攻击）从源头上防止黑客对业务系统后台数据库敏感信息进行非法操作导致敏感信息被泄露的风险。

基于特征识别的文件类型过滤

之所以产生“拖库”的问题，很大一部分原因是由于入侵者通过注入类攻击获取服务器权限之后，可以轻易的将数据库中的敏感信息打包成数据库的文件，通过文件的形式下载到本地。通过对业务系统可输出文件类型的检查，可以很大程度上防御“拖库”事件的产生。

即时的安全审计及短信报警

提供实时的敏感信息内容交互的详细日志，便于日后追查问题的解决。同时提供即时的短信、邮件等方式的报警，便于发现被认为不符合安全策略的访问并采取及时有效的安全应急响应措施。